

Japanese Patent Laid-open Publication No.: 2001-326692 A

Publication date : November 22, 2001

Applicant : HITACHI Ltd.

Title : Interconnecting device and network system using the  
5 same

[0017]

One of the lines is used as an administration line 140 for  
exchanging various setting information among the  
10 interconnecting devices, and the remaining lines are used  
as lines for data 130.

[0028] The administration-information transmitting and  
15 receiving unit 350 obtains setting of the interconnecting  
device from the conversion-table administration unit 320 to  
construct a packet based on a protocol for exchanging the  
setting information between the interconnecting devices,  
and passes the packet to the external line communicating  
20 unit 370. The administration-information transmitting and  
receiving unit 350 receives the packet based on the setting  
exchange protocol between the interconnecting devices from  
the external line communicating unit 370 and interprets it,  
and passes the setting information to the conversion-table  
25 administration unit 320. In some cases, the  
administration-information transmitting and receiving unit  
350 further constructs a return packet of the received  
packet, and passes it to the external line communicating  
unit 370.

30

[0031] The conversion table 325 is stored with protocol  
conversion information of each VPN-ID in a table format, as

shown in Fig. 4. Each conversion information includes: a VPN-ID 410; a partner VPN-ID 420; a connection netmask 430; a router address 440; a partner router address 450; an I/F identifier 460; a sequence number 470; and a flag 480.

5 [0032] The VPN-ID 410 is a number for uniquely identifying each VPN in a service provider to which the interconnecting device belongs, and the partner VPN-ID 420 is the VPN-ID within a service provider of the connecting partner. A VPN represented by the VPN-ID 410 and a VPN  
10 represented by the partner VPN-ID 420 are connected to each other. The connection netmask 430 is a netmask of an IP address assigned to a network between border routers of the both in the VPN-ID, and the router address 440 is an IP address of a border router in the network. The partner  
15 router address 450 is an IP address of a border router on the service provider side of a partner in the network. The I/F identifier 460 is an identifier of an interface used at the time of transmitting and receiving with an interconnecting device of the partner in the VPN-ID.

20

Firstly, the network administrator inputs the VPN-ID, the partner VPN-ID, the connection netmask, and the router address of the border router 120-A, and the I/F identifier  
25 of the interconnecting device 110-A, subject to conversion, into the interconnecting device 110-A (sequence 500).

[0036] (2) The interconnecting device 110-A temporarily registers the inputted information into the conversion table 325, setting the flag to the "waiting for temporary  
30 registration response". Subsequently, the interconnecting device 110-A transmits a VPN registration message including these pieces of information through the administration line to the interconnecting device B (sequence 510).

[0037] (3) The interconnecting device 110-B that receives the message temporarily registers the received transmission-side VPN-ID, receiving-side VPN-ID, connection netmask, transmission-side router address into the  
5 conversion table of its own, setting the flag to the "waiting for registration authorization".

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2001-326692  
(P2001-326692A)

(43)公開日 平成13年11月22日(2001.11.22)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
H 0 4 L	12/66	H 0 4 L 11/20	B 5 K 0 3 0
	12/46	11/00	3 1 0 C 5 K 0 3 3
	12/28	11/20	1 0 2 D
	12/56		

審査請求 未請求 請求項の数6 O L (全 25 頁)

(21)出願番号 特願2000-143779(P2000-143779)

(22)出願日 平成12年 5 月16日(2000. 5. 16)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72)発明者 柘植 宗俊

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 川井 恵理

神奈川県秦野市堀山下 1 番地 株式会社日立製作所エンタープライズサーバ事業部内

(74)代理人 100078134

弁理士 武 顕次郎

Fターム(参考) 5K030 GA11 HA08 HC13 HD03 HD09  
JA11 KA05 LD20 MC08

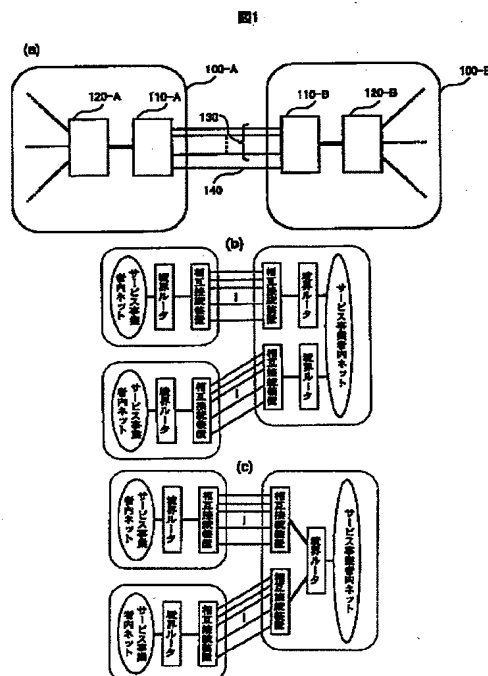
5K033 AA04 AA09 CB09 CC01 DB19

(54)【発明の名称】 相互接続装置及びこれを用いたネットワークシステム

(57)【要約】

【課題】 互いに異なる方式又は識別番号で複数の仮想プライベートネットワーク (VPN) を管理している複数のネットワーク接続サービス事業者の間でVPN単位に相互接続する相互接続装置及び通信ネットワークシステム。

【解決手段】 各サービス事業者に、VPNの識別番号を含む内部ネットワーク用データパケットを送受信する内部ネットワークと、VPNの識別番号を含まないデータパケットを送受信し識別番号毎に異なる回線を持つ外部通信回線130との間で相互にデータパケットを変換する相互接続装置110を設ける。相互接続装置同士は、さらに別の管理用通信回線140によって接続され、互いのVPNの変換情報を交換する。



## 【特許請求の範囲】

【請求項1】 特定のユーザに対して仮想的な専用通信路を提供する複数のネットワーク接続サービス事業者のネットワーク同士を相互接続するために、各ネットワーク接続サービス事業者のネットワーク毎に設置される相互接続装置において、前記特定のユーザを識別するために用いられる識別番号が付与されたデータパケットを第1のネットワークインタフェースから受信し、受信したデータパケットを前記識別番号を取り除いたデータパケットに変換し、変換したデータパケットを、相手側ネットワーク接続事業者との接続を行う前記識別番号毎に割り当てられた第2のネットワークインタフェースへ送信する手段と、前記識別番号のないデータパケットを前記第2のネットワークインタフェースから受信し、第2のネットワークインタフェース毎に割り当てられた前記識別番号を受信したデータパケットに付加し、第1のネットワークインタフェースへ送信する手段と、前記識別番号から対応する第2のネットワークインタフェースを導き出し、第2のネットワークインタフェースから対応する前記識別番号を導き出す前記識別番号と第2のネットワークインタフェースとの対応関係を保持する手段と、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置との間で通信を行って、前記識別番号と第2のインタフェースとの対応関係を交換する手段とを備えることを特徴とする相互接続装置。

【請求項2】 管理者が入出力装置を通して、あるいは、管理者が操作する装置との間で通信を行って、前記識別番号と第2のネットワークインタフェースとの対応関係を追加または削除する手段とを備えたことを特徴とする請求項1記載の相互接続装置。

【請求項3】 管理者が入出力装置を通して、あるいは、管理者が操作する装置との間で通信を行って、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置から受信した前記識別番号と第2のネットワークインタフェースとの対応関係に関する情報を確認し、これを設定することを承認する手段を備えたことを特徴とする請求項2記載の相互接続装置。

【請求項4】 前記識別番号付きデータパケットを送受信する第1のネットワークインタフェースに接続された装置に対して、前記識別番号に対応した通信に必要な情報を通知する手段を備えたことを特徴とする請求項1、2または3記載の相互接続装置。

【請求項5】 複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、請求項1ないし4のうちのいずれか1記載の相互接続装置と、他の通信ネットワークの相互接続装置との間を接続し、識別

番号なしデータパケットを用いて通信を行う手段とを備えることを特徴とする通信ネットワークシステム。

【請求項6】 複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、前記識別番号なしのデータパケットを用いて他の通信ネットワークの相互接続装置との通信を行い、前記識別番号付きのデータパケットを用いて通信を行うネットワークと前記識別番号なしのデータパケットを用いた他の通信ネットワークとを相互に接続する請求項1ないし4のうちのいずれか1記載の相互接続装置とを備えることを特徴とする通信ネットワークシステム。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、相互接続装置及びこれを用いた通信ネットワークシステムに係り、特に、それぞれが独自の方式で仮想的なプライベートネットワークのサービスを行っている複数のネットワークシステム相互間において、各ネットワークシステム内の独自形式のデータと相互接続用の外部共通形式のデータとの間でデータの変換を行い、それによって各ネットワークシステム相互間でプライベートネットワークの相互接続可能にする相互接続装置及びこれを用いた通信ネットワークシステムに関する。

## 【0002】

【従来の技術】近年、急速なネットワークの普及等により、出張先やサテライトオフィスからネットワーク接続サービス事業者（以下、単にサービス事業者という）の回線を通して会社へ接続するという需要が増加している。それに伴い、出張先やサテライトオフィスと会社との間の接続をあたかもローカルエリアネットワークのように扱うことを可能にして、互いに遠隔接続したユーザホスト間の連携を容易にすると共に、それ以外のホストとの間のセキュリティを確保する、いわゆる仮想プライベートネットワーク（Virtual Private Network、以下、VPNという）が注目されるようになってきている。

【0003】前述のような互いに遠隔地にあるユーザホスト相互間でVPNを構築する方法として、次に説明するような2つの方法が考えられる。第1の方法は、インターネットのような広範囲の地域を網羅しているが信頼性の低い伝送路上で、伝送パケットを暗号化する等により、信頼性のある仮想的な接続を構築するという方法である。第2の方法は、単一のサービス事業者が自らのネットワークを使用した信頼性の高い伝送路内のみにおいて独自のプライベートネットワークサービスを提供している場合、このネットワークを利用するという方法である。このようなネットワークの例として、例えば、NT

T R&D1998年4月号で紹介されている次世代コネクションレスネットワーク等が知られている。

【0004】前述の第1の方法は、サービス事業者側がVPNのための機構を導入する必要がほとんどないことや、各ユーザホストが単一のサービス事業者に接続している必要がなく、接続の自由度が高いため、サービス事業者、ユーザ両方にとってネットワーク接続自体のコストが安くなるというメリットを有している。しかし、この第1の方法は、ユーザ側でVPN構築のためのソフトウェアを導入する必要が有ること、通信時に必ず暗号化・復号化を伴うこと、インターネットの通信品質が保証されていないこと等の理由により、ユーザ側のホスト管理コストや通信品質の点で第2の方法に劣るものである。一方、第2の方法は、逆に、通信品質やホスト管理コストの点で、第1の方法より優れているが、各ユーザホストが単一のサービス事業者に接続しなければならないため、接続できる地理的範囲が限られるものである。

#### 【0005】

【発明が解決しようとする課題】VPNは、ローカルエリアネットワークを遠隔地へ拡張したものであると考えることができ、可能な限りローカルエリアネットワーク環境に近い、あるいは、それよりも便利な環境を構築することができることが望ましい。このためには、VPNの環境を、コスト、品質の両面でローカルエリアネットワーク環境に少しでも近づける必要があり、前述した従来技術の欠点の改善が必要である。

【0006】前述した第1の方法におけるインターネット上の伝送信号を暗号化して伝送する手法の欠点である「ユーザ側のホスト管理コスト」及び「通信品質」の改善方法として、VPN用のソフトウェアの設定等の簡易化や、インターネットそのものの通信速度の改善、通信品質の保証を実現することが考えられる。

【0007】また、前述した第2の方法における単一サービス事業者が提供する独自プライベートネットワークサービスを用いる手法の欠点である「接続できる地理的範囲の制限」については、自らのネットワーク内でVPNサービスを行っており、通信品質について信頼できるサービス事業者の複数の事業者同士が、ユーザの要望に応じてVPNの相互接続を行うという方法によりある程度緩和することができる。

【0008】しかし、VPNの実現方法については統一された規格がないため、前述した第2の方法における複数の事業者同士がVPNの相互接続を行うという方法は、それぞれのサービス事業者側でVPNの仕様が異なることが考えられ、また、両サービス事業者のVPNの仕様が同一の場合でも、ネットワーク管理者がサービス事業者毎に異なるため、各VPNを一意に識別するために用いているID番号等が互いに食い違っている場合も考えられるため、単純には相互接続することができないという問題点を有している。

【0009】一方、前述した第1の方法を用いる場合の問題点は、異種VPN相互間の中継方法に関する技術として、例えば、特開平11-41280号公報等に記載された技術により解決されている。しかし、この公報に記載された技術は、1つのサービス事業者が同一のネットワーク上で複数のVPNを提供するという前述した第2の方法が前提としているような場合を想定していないため、第2の方法におけるVPN相互接続装置として適用することが難しいという問題点を有している。

10 【0010】本発明の目的は、前述した第2の方法におけるVPNの仕様やID番号の相違に関する問題点を解決し、異なるサービス事業者のVPN相互を効率的に接続することを可能にした相互接続装置及びこれを用いたネットワークシステムを提供することにある。

#### 【0011】

【課題を解決するための手段】本発明によれば前記目的は、複数のサービス事業者が相手のサービス事業者のネットワークとの接続回線上にVPN相互接続装置を設置し、サービス事業者内部におけるVPNのID番号を含んだパケットと、相手のサービス事業者との間で送受信するサービス事業者で統一された形式のパケットとの間で変換を行うようにすることにより達成される。

20 【0012】すなわち、本発明によれば前記目的は、特定のユーザに対して仮想的な専用通信路を提供する複数のネットワーク接続サービス事業者のネットワーク同士を相互接続するために、各ネットワーク接続サービス事業者のネットワーク毎に設置される相互接続装置において、前記特定のユーザを識別するために用いられる識別番号が付与されたデータパケットを第1のネットワークインタフェースから受信し、受信したデータパケットを前記識別番号を取り除いたデータパケットに変換し、変換したデータパケットを、相手側ネットワーク接続事業者との接続を行う前記識別番号毎に割り当てられた第2のネットワークインタフェースへ送信する手段と、前記識別番号のないデータパケットを前記第2のネットワークインタフェースから受信し、第2のネットワークインタフェース毎に割り当てられた前記識別番号を受信したデータパケットに付加し、第1のネットワークインタフェースへ送信する手段とを備えることにより達成される。

40 【0013】また、前記目的は、複数の通信ネットワーク相互間を相互に接続して構成される通信ネットワークシステムにおいて、前記複数の通信ネットワークのそれぞれは、通信を行っている特定のユーザを識別する識別番号付きのデータパケットを用いて通信を行い、互いに前記識別番号を独立して管理している複数のネットワークと、前述の相互接続装置と、他の通信ネットワークの相互接続装置との間を接続し、識別番号なしデータパケットを用いて通信を行う手段とを備えることにより達成される。

【0014】相互接続装置の相互間は、物理的あるいは論理的に複数の回線が引かれており、この回線の1つ毎に1つのVPNが対応する。このようにすることで、相手のサービス事業者との送受信に使われるパケットにはVPNに関する情報が不用になるので、例えば、一般的なIPパケット形式を互いの送受信に用いるパケット形式として採用することができる。さらに、当該するVPNを用いているユーザが常にIPのパケット形式を用いて送受信を行っていれば、各サービス事業者はVPNを実現するために付加した余分な情報を取り払うだけでサービス事業者相互送受信用のパケット形式であるIPパケットへ変換することができる。

#### 【0015】

【発明の実施の形態】以下、本発明による相互接続装置及びこれを用いたネットワークシステムの実施形態を図面を用いて詳細に説明する。

【0016】図1は本発明の相互接続装置を用いてサービス事業者間のVPN相互接続を行うネットワークシステムの構成例を示すブロック図である。図1において、100-A、100-Bはサービス事業者ネットワーク、110-A、110-Bは相互接続装置、120-A、120-Bは境界ルータ、130はデータ用回線、140は管理用回線である。

【0017】図1(a)に示すシステムは、2者のサービス事業者ネットワーク100-A、100-Bの相互間が各サービス事業者内に置かれた相互接続装置110-A、110-Bにより接続されて構成される。そして、それらの相互接続装置は、各サービス事業者内の境界ルータ120-A、120-Bに第1のネットワークインタフェースとしての回線により接続されている。この図1(a)に示す構成は、本発明の実施形態によるネットワークシステムの最も基本的な構成である。図示システムの特徴をなす装置である相互接続装置110-Aと110-Bとの間は、OSI参照モデルにおける物理層あるいはデータリンク層のレベルで個別に分けることができる複数の回線による第2のネットワークインタフェースで接続されている。それらの回線の内の1つは、相互接続装置相互間で各種の設定情報を交換するための管理用回線140として使用され、残りの回線は、データ用回線130として使用される。境界ルータ120-A、120-Bは、さらに、各サービス事業者ネットワーク内のルータ、サービス事業者がサービス対象とするユーザのネットワーク、他の外部ネットワーク等と接続されている。

【0018】相互接続装置110-A、110-Bは、相手のサービス事業者の相互接続装置への中継、あるいは、相手のサービス事業者の相互接続装置からの中継を行うべきVPNを管理し、それらの情報をネットワーク管理者や相手のサービス事業者の相互接続装置へ伝達する。また、相互接続装置110-A、110-Bは、そ

れらのVPNのパケットを境界ルータ120-A、120-Bとの間で送受信できるように境界ルータ間のネットワーク設定を各境界ルータへ送信し、境界ルータや相手の相互接続装置から送られてくる各パケットのうち不正なものを破棄した上で反対側へ中継する。

【0019】なお、相互接続装置は、受信したパケットをVPN-ID(VPNを一意に識別する番号)及びVPN-IDと対応させたデータ用回線130のみに基づいて転送し、パケットに含まれるIPアドレスについては関知しない。このため、IPアドレスに基づくパケットのルーティングは、境界ルータ120-A、120-Bが行う。

【0020】図1(b)、図1(c)に示す例は、サービス事業者ネットワークを2つ以上とした場合の構成例である。サービス事業者ネットワークを2つ以上とした場合のネットワークシステムは、図1(b)に示すように、各サービス事業者ネットワーク内に接続相手毎に相互接続装置と境界ルータとを備える構成とすることが基本である。また、図1(c)に示すように、2つ以上の接続相手に対して共通の境界ルータを設け、その境界ルータから接続相手毎に別々のネットワークインタフェースを用い、接続相手毎に設けた別々の相互接続装置を介して相手のサービス事業者と接続するという構成であってもよい。但し、いずれの場合も、境界ルータは、受信したデータパケットをその宛先のIPアドレスへ向かうネットワークインタフェースのみに対して適切に転送することができる機能を備える必要がある。これは、後述するように、本発明による相互接続装置が、データパケット転送時にVPN識別番号のみに関与し、データパケットの送信元IPアドレス、宛先IPアドレスについて関知しないことを前提としているためである。

【0021】図2は本発明の一実施形態による相互接続装置のハードウェア構成を示すブロック図、図3は本発明の一実施形態による相互接続装置のソフトウェア構成を説明する図、図4は本発明の一実施形態による相互接続装置が使用する変換テーブルの構成を説明する図である。図2～図4において、200はCPU(Central Processing Unit)、210はメモリ、213はオペレーティングシステム(OS)、215は制御ソフト、220は内部ネットワークコントローラ、225は外部ネットワークコントローラ、230はキーボードコントローラ、235はキーボード、240はシリアルコントローラ、245はマウス、250はディスプレイコントローラ、255はディスプレイモニタ、260はディスクコントローラ、265はディスク装置、310は入出力制御部、320は変換管理テーブル、325は変換テーブル、330は境界ルータ接続設定部、340はデータ中継部、350は管理情報送受信部、360は境界ルータ通信部、370は外部回線通信部、380は内部ネットワークインタフェース部、390は外部ネットワークイ

インタフェース部である。

【0022】相互接続装置110は、図2に示すようなハードウェア構成を持ち、CPU200がメモリ210に格納されているプログラムを実行する。メモリ210の中には、装置全体を制御するためのOS213、相互接続装置としての動作を行うための制御プログラム215が格納されている。内部ネットワークコントローラ220は、相互接続装置が境界ルータとの間で行う送受信を制御し、外部ネットワークコントローラ225は、相互接続装置が相手のサービス事業者の相互接続装置との間で行う送受信を制御する。キーボードコントローラ230は、キーボード235からのキー入力を制御し、シリアルコントローラ240は、シリアルポートに接続されたマウス245等の入出力機器を制御する。また、ディスプレイコントローラ250は、ディスプレイモニタ255への画面表示を制御し、ディスクコントローラ260は、ディスク装置265への入出力を制御する。

【0023】図示本発明の実施形態は、ネットワーク管理者による相互接続装置の操作を、装置に直接接続されたキーボード235、マウス245、ディスプレイモニタ255から行うことを前提とするが、相互接続装置とネットワークとを介して接続された遠隔地にある入出力装置を用いて操作を行うことも可能である。

【0024】制御プログラム215内に構成される相互接続装置のソフトウェア構成を図3に示している。図3において、入出力制御部310は、キーボード235からの入力やディスプレイモニタ255への出力を制御する。内部ネットワークインタフェース部380は、境界ルータに接続されたネットワークから受信したパケットを境界ルータ通信部360に渡したり、境界ルータ通信部360からの要求によりパケットをそのネットワークに送信する等の境界ルータとの間の送受信に関する処理を行う。外部ネットワークインタフェース部390は、相手のサービス事業者の相互接続装置に接続されたネットワークから受信したパケットを外部回線通信部370に渡したり、外部回線通信部370から渡されたパケットを要求された通りのネットワークに送信する等の相手の相互接続装置との間の送受信に関する処理を行う。

【0025】境界ルータ通信部360は、内部ネットワークインタフェース部380から受け取ったパケットのヘッダを解釈し、その結果に応じて境界ルータ接続設定部330、データ中継部340のうちの適切な処理モジュールの方へパケットを渡したり、これらの処理モジュールから渡されたパケットに適切なヘッダを付加して内部ネットワークインタフェース部380へ渡す等の内部プロトコルに応じたパケットヘッダの解釈と各モジュールへのパケット振分処理とを行う。

【0026】外部回線通信部370は、外部ネットワークインタフェース部390から受け取ったパケットをその受信回線に応じて、管理情報送受信部350、データ

中継部340のうちの適切な処理モジュールの方へ渡したり、これらの処理モジュールから渡されたパケットに適切な送信回線の要求を付加して外部ネットワークインタフェース部へ渡す等の外部回線と各モジュールとの間でのパケット振分処理を行う。

【0027】境界ルータ接続設定部330は、境界ルータに与えるべき設定が入出力制御部310から管理者により入力されるか、あるいは、管理情報送受信部を通して相手の相互接続装置から与えられると、それらの設定を変換テーブル管理部320を通して受け取り、設定情報を境界ルータへ送るための適切な通信手順に基づいてパケットに構築し、境界ルータ通信部360へ受け渡す。但し、このような通信による設定手段が境界ルータに備わっていない場合、管理者が手動で境界ルータに設定を行うことによって対処することができる。

【0028】管理情報送受信部350は、相互接続装置の設定を変換テーブル管理部320から得て、相互接続装置間での設定情報交換のためのプロトコルに基づいてパケットを構築し、外部回線通信部370へ受け渡す。

また、管理情報送受信部350は、相互接続装置間の設定交換プロトコルに基づくパケットを外部回線通信部370から受け取って解釈し、その設定情報を変換テーブル管理部320に受け渡し、さらに場合によっては受信パケットの返答パケットを構築して外部回線通信部370へ受け渡す。

【0029】データ中継部340は、境界ルータ通信部360から受け取ったパケットに含まれるVPN-IDを変換テーブル管理部320に渡して登録されているか否かを調べ、中継対象として登録されている場合、そのパケットの形式を外部の相互接続装置との間の通信形式であるIPパケットに変換し、送出すべきインタフェースの識別子を付加して外部回線通信部370に渡す。また、データ中継部340は、外部回線通信部370からIPパケットを受け取ると、そのパケットが流れてきたインタフェースの識別子を変換テーブル管理部320に渡して登録されているか否かを調べ、中継対象として登録されている場合、そのパケットの形式を境界ルータとの間の通信形式のパケットに変換し、そのパケット内に変換後のVPN-ID番号を書き込んで境界ルータ通信部360に渡す。

【0030】変換テーブル管理部320は、変換テーブル325を管理し、入出力制御部310、境界ルータ接続設定部330、データ中継部340、管理情報送受信部350からの変換テーブル内の情報の追加、削除、検索等の要求を受け付け、それらの要求に基づいて変換テーブルを操作し、検索結果等の返答を要求元モジュールへ返す。

【0031】変換テーブル325には、図4に示すように、各VPN-IDのプロトコル変換情報がテーブル形式で格納されている。各変換情報には、VPN-ID4



10、相手VPN-ID420、接続ネットマスク430、ルータアドレス440、相手ルータアドレス450、I/F識別子460、シーケンス番号470、フラグ480が含まれる。

【0032】VPN-ID410は、この相互接続装置が属するサービス事業者内において、各VPNを一意に識別するための番号であり、相手VPN-ID420は、接続相手のサービス事業者内におけるVPN-IDである。これらの、VPN-ID410で表されるVPNと、相手VPN-ID420で表されるVPNとが相互に接続されることとなる。接続ネットマスク430は、そのVPN-IDにおける両者の境界ルータ間のネットワークに割り振るIPアドレスのネットマスクであり、ルータアドレス440は、そのネットワークにおける境界ルータのIPアドレスである。相手ルータアドレス450は、そのネットワークにおいて相手のサービス事業者側にある境界ルータのIPアドレスである。I/F識別子460は、そのVPN-IDにおいて相手の相互接続装置との間で送受信する際に用いるインタフェースの識別子である。シーケンス番号470は、相互接続装置同士が交換した管理メッセージを一意に識別するためのシーケンス番号を一時的に格納するために用いられる。フラグ480は、管理メッセージの交換状態を表すために用いられる状態フラグであり、フラグ480が表す状態には、「仮登録返待ち」、「登録完了待ち」、「登録承認待ち」、「削除承認待ち」、「有効」の5種類がある。相互接続装置は、受信したパケットのVPN-IDが「有効」として変換テーブルに登録されている場合にのみ、そのパケットの転送を行う。

【0033】なお、前述したテーブルの内容、特に、VPN-IDの識別番号と相手側相互接続装置に接続される回線を示すI/F識別子のネットワークインタフェースとの対応関係等については、管理者が入出力装置を通して、あるいは、管理者が操作する図示しない装置との間で通信を行って、追加または削除することができる。また、管理者は、他のネットワーク接続サービス事業者のネットワークに設置された相互接続装置から受信した前述の情報を確認し、入出力装置を通して、あるいは、管理者が操作する図示しない装置との間で通信を行って、これを設定することを承認するようにすることができる。

【0034】図5は相互接続装置相互間のVPN変換情報の登録シーケンスを示しており、以下、これについて説明する。図5に示すシーケンスは、相互接続装置110-A側のネットワーク管理者の要求による登録処理を示しているが、相互接続装置110-B側からの要求の場合も同様である。

【0035】(1) 要求を出す相互接続装置110-A側のネットワーク管理者は、互いに接続したい相互接続装置110-A側のVPN-ID、相互接続装置110

ーB側のVPN-ID、境界ルータ間の相互接続に利用できるIPネットワークアドレスを予め把握していることとする。まず、ネットワーク管理者は、相互接続装置110-Aに対して変換の対象となるVPN-ID、相手VPN-ID、接続ネットマスク、境界ルータ120-Aのルータアドレス、及び、相互接続装置110-AのI/F識別子を入力する(シーケンス500)。

【0036】(2) 相互接続装置110-Aは、入力された情報を、フラグを「仮登録返待ち」にして変換テーブル325に仮登録する。そして、それらの情報を含むVPN登録メッセージを相互接続装置Bへ管理用回線を通して送信する(シーケンス510)。

【0037】(3) このメッセージを受信した相互接続装置110-Bは、自らの変換テーブルへ受信した送信側VPN-ID、受信側VPN-ID、接続ネットマスク、送信側ルータアドレスを、フラグを「登録承認待ち」にして仮登録する。また、相互接続装置110-Bは、相手の相互接続装置のI/F識別子から、その回線に接続されている自らのI/F識別子を導き出し、仮登録した変換情報のI/F識別子フィールドに登録する。相互接続装置110-Bは、相互接続装置110-Aから要求されたVPN変換情報の仮登録処理が終わると、相互接続装置110-Aに対して管理用回線を通して仮登録完了を表すACKメッセージを送信する(シーケンス520)。

【0038】(4) このメッセージを受信した相互接続装置110-Aは、対象となる変換情報のフラグを「登録完了待ち」へ変更する。その後、相互接続装置110-Bは、仮登録された変換情報の登録承認及び追加情報の入力が相互接続装置110-B側のネットワーク管理者によって行われるまで待ち状態となる。但し、データパケットの変換処理及び他のVPNに関する変換情報登録、削除の処理については、この入力待ちとは無関係に並行して処理することができる(シーケンス530)。

【0039】(5) 相互接続装置110-Bは、シーケンス530により相互接続装置110-B側のネットワーク管理者によってVPN変換情報設定の登録承認及び境界ルータ120-Bのルータアドレスが入力されると、次のシーケンス以降の処理に移る。但し、相互接続装置110-A側と110-B側のネットワーク管理者が同一の場合、シーケンス530及びその入力待ち処理を省略し、境界ルータ120-Bのルータアドレスも相互接続装置110-A側のネットワーク管理者がシーケンス500で与えるようにすることができる。シーケンス530でネットワーク管理者による承認が与えられると、相互接続装置110-Bは、まず、境界ルータBに対してアドレス設定等のデータの送受信やルーティングプロトコルの交換に必要な設定を行う。但し、この設定を相互接続装置110-Bが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ120-

Bに対してこれらの設定を行ってもよい（シーケンス540）。

【0040】（6）境界ルータ120-Bに対するシーケンス540での設定が終わると、相互接続装置110-Bは、変換テーブル内の該当する変換情報のフラグを「有効」へ変更し、登録完了メッセージを相互接続装置110-Aに対して管理用回線を通して送信する（シーケンス550）。

【0041】（7）登録完了メッセージを受信した相互接続装置110-Aは、境界ルータ120-Aに対してアドレス設定等のデータ送受信やルーティングプロトコルの交換に必要な設定を行う。但し、この設定を相互接続装置110-Aが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ120-Aに対してこれらの設定を行ってもよい（シーケンス560）。

【0042】（8）相互接続装置110-Aは、境界ルータ120-Aに対するシーケンス560での設定が終わると、変換テーブル内の該当する変換情報のフラグを「有効」へ変更し、相互接続装置110-Bに対して管理用回線を通して登録完了を表すACKメッセージを送信する（シーケンス570）。

【0043】図6は相互接続装置相互間のVPN変換情報の削除シーケンスを示しており、以下、これについて説明する。図6に示すシーケンスは、相互接続装置110-A側のネットワーク管理者の要求による削除処理を示しているが、相互接続装置110-B側からの要求の場合も同様である。

【0044】（1）要求を出す相互接続装置110-A側のネットワーク管理者は、まず、相互接続装置110-Aに対して、変換テーブルから削除したいVPN-IDを入力する。相互接続装置110-Aは、入力されたVPN-IDと一致する変換情報を変換テーブルから検索し、見つかった変換情報に基づいて境界ルータ120-Aに対してアドレス削除等のデータ送受信やルーティングプロトコルの交換の中止に必要な設定を行う。但し、この設定を相互接続装置110-Aが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータ120-Aに対してこれらの設定を行ってもよい（シーケンス600、610）。

【0045】（2）シーケンス610の処理後、相互接続装置110-Aは、該当するVPN-IDの削除メッセージを相互接続装置110-Bに対して管理用回線を通して送信し、該当する変換情報を変換テーブルから削除する（シーケンス620）。

【0046】（3）シーケンス620によるメッセージを受信した相互接続装置110-Bは、自らの変換テーブルから受信した受信側VPN-IDを検索し、見つかった変換情報のフラグを「削除承認待ち」にすることによって変換情報を仮削除し、相互接続装置110-Aに対して管理用回線を通して仮削除完了を表すACKメッ

ッセージを送信する（シーケンス630）。

【0047】（4）その後、相互接続装置110-Bは、仮削除された変換情報の削除承認が相互接続装置B側のネットワーク管理者によって行われるまで入力待ち状態となる。但し、データパケットの変換処理及び他VPNに関する変換情報の登録処理、削除処理については、この入力待ちとは無関係に並行して処理することができる（シーケンス640）。

【0048】（5）相互接続装置110-Bは、シーケンス640により削除の承認が入力されると、次のシーケンスの処理に移る。但し、相互接続装置110-A側と110-B側とのネットワーク管理者が同一の場合、シーケンス640及びその入力待ち処理を省略することができる。シーケンス640でネットワーク管理者による承認が与えられると、相互接続装置110-Bは、境界ルータ120-Bに対してアドレス削除等のデータ送受信やルーティングプロトコルの交換の中止に必要な設定を行う。但し、この設定を相互接続装置110-Bが自動的に行うことができない場合、ネットワーク管理者が直接境界ルータBに対してこれらの設定を行ってもよい。境界ルータ120-Bに対する設定が終了すると、相互接続装置110-Bは、変換テーブル内の該当する変換情報を完全に削除する（シーケンス650）。

【0049】図7は相互接続装置相互間でのデータパケットの送受信シーケンスを示しており、以下、これについて説明する。図7に示すシーケンスは、相互接続装置110-A側からのデータパケットの送信処理を示しているが、相互接続装置110-B側からの送信の場合も同様である。

【0050】（1）相互接続装置110-Aは、境界ルータ120-Aから送信すべきパケットを受け取ると、そのヘッダに含まれるVPN-IDを変換テーブルから検索する。その結果、変換テーブルに該当する変換情報が存在し、かつ、そのフラグが「有効」であるならば、そのデータパケットからサービス事業者内部での送受信のために付けられているヘッダ（VPN-IDを含む）を取り除いて、相互接続装置110-Bに対してVPN-IDに対応するデータ用回線を用いて送信する（シーケンス700、710）。

【0051】（2）相互接続装置110-Aからデータパケットを受信した相互接続装置110-Bは、受信したデータ用回線のI/F識別子を変換テーブルから検索する。その結果、該当する変換情報が存在し、かつ、そのフラグが「有効」であるならば、その変換情報のVPN-IDを含むサービス事業者内部用ヘッダをそのパケットに付加し、境界ルータ120-Bへ転送する（シーケンス720）。

【0052】図8はVPN変換情報を登録しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する登録メッセージの形式を示す図であり、図5

により説明したシーケンス510で送信されるメッセージである。

【0053】図8に示すように、登録メッセージ800は、メッセージ長等を含むメッセージヘッダであるヘッダ805と、以下に説明する各種の情報810～870により構成される。シーケンス番号810は、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられる。送信側外部I/F識別子820は、このメッセージを送信する側の相互接続装置における該当VPN-IDに対応するインタフェース識別子である。送信側内部VPN-ID830は、このメッセージを送信する側のサービス事業者内におけるVPN-IDである。受信側内部VPN-ID840は、このメッセージを受信する側のサービス事業者内におけるVPN-IDである。最終的に、この送信側内部VPN-ID830で表されるVPNと受信側内部VPN-ID840で表されるVPN同士が互いに接続されることになる。ルータ間接続IPネットマスク850は、境界ルータ間のネットワークのIPネットマスクである。送信側ルータIPアドレス860は、境界ルータ間の接続において送信側の境界ルータに割り当てたIPアドレスである。受信側ルータIPアドレス870は、境界ルータ間の接続において受信側の境界ルータに割り当てるIPアドレスである。但し、受信側のネットワーク管理者が受信側の境界ルータに割り当てるIPアドレスを決定する場合、この受信側ルータIPアドレスのフィールドは空でもよい。

【0054】図9は登録メッセージを受信した相互接続装置が登録メッセージを送信してきた相互接続装置へ返信する登録完了メッセージの形式を示す図であり、図5により説明したシーケンス550で送信されるメッセージである。

【0055】図9に示すように、登録完了メッセージ900は、メッセージ長等を含むメッセージヘッダであるヘッダ905と、以下に説明する各種の情報910～970により構成される。

【0056】シーケンス番号910は、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられる。仮設定シーケンス番号920は、このメッセージが返答の対象としている登録メッセージのシーケンス番号である。送信側内部VPN-ID930は、このメッセージを送信する側のサービス事業者内におけるVPN-IDである。受信側内部VPN-ID940は、このメッセージを受信する側のサービス事業者内におけるVPN-IDである。この送信側内部VPN-ID930で表されるVPNと受信側内部VPN-ID940で表されるVPN同士が互いに接続されたことになる。ルータ間接続IPネットマスク950は、境

界ルータ間のネットワークのIPネットマスクである。送信側ルータIPアドレス960は、境界ルータ間の接続において送信側の境界ルータに割り当てたIPアドレスである。受信側ルータIPアドレス970は、境界ルータ間の接続において受信側の境界ルータに割り当てたIPアドレスである。

【0057】図10はVPN変換情報を削除しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する削除メッセージの形式を示す図であり、図6により説明したシーケンス620で送信されるメッセージである。

【0058】図10に示すように、削除メッセージ1000は、メッセージ長等を含むメッセージヘッダであるヘッダ1005と、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられるシーケンス番号1010と、このメッセージを受信する側のサービス事業者内におけるVPN-IDである受信側内部VPN-ID1020とにより構成される。そして、VPN-IDで指定された変換情報が両側の相互接続装置の変換テーブルから削除される。

【0059】図11は図8～図10のメッセージを受け取った相互接続装置が相手の相互接続装置へ返答する受信確認(ACK)メッセージの形式を示す図である。

【0060】ACKメッセージ1100は、メッセージ長等を含むメッセージヘッダであるヘッダ1105と、このACKメッセージが返答の対象としているメッセージのシーケンス番号である返答対象シーケンス番号1110と、このメッセージを受信する側のサービス事業者内におけるVPN-IDである受信側内部VPN-ID1120とにより構成される。ACKメッセージは、返答対象メッセージのシーケンス番号のみを持ち、ACKメッセージ自身のシーケンス番号を持たない。そして、前述の受信側内部VPN-ID1120は、返答対象のメッセージが指定したVPN-IDと対応させられている。

【0061】図12は相互接続装置がメッセージの受け取り時にエラーが発生した場合に相手の相互接続装置へ送信する異常通知(NOTIFY)メッセージの形式を示す図である。

【0062】NOTIFYメッセージ1200は、メッセージ長等を含むメッセージヘッダであるヘッダ1205と、管理用回線を流れる各メッセージを一意に区別するための番号で、今までに流れたメッセージのシーケンス番号と可能な限り異なる値が用いられるシーケンス番号1210と、このメッセージを受信する側のサービス事業者内におけるVPN-IDである受信側内部VPN-ID1220と、このNOTIFYメッセージが相手の相互接続装置へ伝えるエラーの種別を表すエラーコード1230と、エラーの内容を表すための付加的なパラ

メータであるエラーパラメータ1240とにより構成される。前述の受信側内部VPN-ID1220は、このNOTIFYメッセージがエラーの対象とするVPN-IDと対応させられている。

【0063】図13はVPN変換情報を登録しようとしたサービス事業者側の相互接続装置における変換情報仮登録の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、前述の図5のシーケンス500でネットワーク管理者の登録要求を受け取った相互接続装置110-Aが、フラグを「仮登録返答待ち」にして、入力された情報を変換テーブル325に仮登録し、シーケンス510で登録メッセージを送信するまでの処理に相当する。

【0064】(1) ネットワーク管理者からVPN変換情報の新規登録要求が入力された相互接続装置は、自VPN-IDが一致する変換情報を変換テーブルから検索し、検索の結果、要求されたVPN-IDが自装置の変換テーブルにすでに登録されているか否かチェックする(ステップ1305、1310)。

【0065】(2) ステップ1310のチェックで、もし変換テーブルに要求されたVPN-IDがあれば、ネットワーク管理者が使用しているディスプレイモニターを出力してここでの処理を終了す(ステップ1325)。

【0066】(3) ステップ1310のチェックで、変換テーブルに要求されたVPN-IDがなければ、ネットワーク管理者によって入力された自サービス事業者側の変換対象VPN-ID、相手サービス事業者側のVPN-ID、境界ルータ間接続のIPネットマスク、自サービス事業者側の境界ルータのIPアドレス、及び、自サービス事業者側相互接続装置のI/F識別子を変換テーブルへ新たな変換情報として登録する。さらに、その変換情報のシーケンス番号に、後のステップ1320で送信する登録メッセージのシーケンス番号を登録し、フラグに、「仮登録返答待ち」を表すフラグ値を登録する(ステップ1315)。

【0067】(4) そして、各フィールドにステップ1315で登録したものと同じ値を持つ登録メッセージ(但し、相手サービス事業者側のルータIPアドレスがネットワーク管理者から指定された場合は、そのフィールドもさらに含む)を相手サービス事業者側の相互接続装置に対して管理用回線経由で送信してここでの処理を終了する(ステップ1320)。

【0068】図14はVPN変換情報を削除しようとしたサービス事業者側の相互接続装置における変換情報削除の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図6において、シーケンス600でネットワーク管理者の削除要求を受け取った相互接続装置110-Aが、シーケンス620で削除メッセージを送信し、削除を要求された情報を変換

テーブル325から削除するまでの処理に相当する。

【0069】(1) ネットワーク管理者からVPN変換情報の削除要求を入力された相互接続装置は、自VPN-IDが一致する変換情報を変換テーブルから検索し、検索の結果、要求されたVPN-IDがすでに変換テーブルに登録されているか否かをチェックする(ステップ1405、1410)。

【0070】(2) ステップ1410のチェックで、もし変換テーブルに要求されたVPN-IDがなければ、ネットワーク管理者が使用しているディスプレイモニターを出力してここでの処理を終了す(ステップ1430)。

【0071】(3) ステップ1410のチェックで、変換テーブルに要求されたVPN-IDがあれば、自サービス事業者側の境界ルータに対して、変換情報に含まれる各種情報(自サービス事業者側と相手サービス事業者側の境界ルータのIPアドレス、境界ルータ間接続のIPネットマスク)やその他ルーティング情報交換のための設定の解除要求を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が削除要求入力を行う前に、他の手段で境界ルータに対して直接この設定解除を行ってもよい(ステップ1415)。

【0072】(4) 次に、対象となっている変換情報に登録されている相手VPN-IDを受信側内部VPN-IDに持つ削除メッセージを、相手サービス事業者側の相互接続装置へ管理用回線経由で送信し、対象となっている変換情報を完全に削除してここでの処理を終了する(ステップ1420、1425)。

【0073】図15は登録メッセージを受信した相互接続装置における変換情報仮登録の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図5において、相互接続装置110-Bが、シーケンス510で登録メッセージを受信してからシーケンス520でACKメッセージを送信するまでの処理に相当する。

【0074】(1) 相手サービス事業者側の相互接続装置から登録メッセージを受信した相互接続装置は、そのメッセージに含まれる受信側VPN-IDに一致する変換情報を変換テーブルから検索し、検索の結果、要求された受信側VPN-IDが自装置の変換テーブルにすでに登録されているか否かチェックする(ステップ1505、1510)。

【0075】(2) ステップ1510のチェックで、もし変換テーブルに要求された受信側VPN-IDがあれば、相手サービス事業者側の相互接続装置へ、エラーを表すNOTIFYメッセージを送信してここでの処理を終了す(ステップ1525)。

【0076】(3) ステップ1510のチェックで、変換テーブルに要求された受信側VPN-IDがなけれ

ば、登録メッセージに含まれる送信側の交換対象VPN-ID、受信側のVPN-ID、境界ルータ間接続のIPネットマスク、送信側の境界ルータのIPアドレスを交換テーブルへ新たな交換情報として登録する。さらに、その交換情報のI/F識別子に、メッセージ内に含まれる送信側外部I/F識別子から導き出した受信側相互接続装置のI/F識別子を登録し、シーケンス番号に、登録メッセージのシーケンス番号を登録し、フラグに、「登録承認待ち」を表すフラグ値を登録する（ステップ1515）。

【0077】（4）そして、仮登録完了を表すACKメッセージを相手サービス事業者側の相互接続装置にたいして管理用回線経由で送信してここでの処理を終了する（ステップ1520）。

【0078】図16は削除メッセージを受信した相互接続装置における交換情報仮削除の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図6において、相互接続装置110-Bが、シーケンス620で削除メッセージを受信してからシーケンス630でACKメッセージを送信するまでの処理に相当する。

【0079】（1）相手サービス事業者側の相互接続装置から削除メッセージを受信した相互接続装置は、そのメッセージに含まれる受信側VPN-IDが交換テーブルにすでに登録されているか否かを検索し、検索の結果、削除すべき受信側VPN-IDがすでに交換テーブルに登録されているか否かをチェックする（ステップ1605、1610）。

【0080】（2）ステップ1610のチェックで、もし交換テーブルに受信側VPN-IDがなければ、相手サービス事業者側の相互接続装置へ未登録エラーを表すNOTIFYメッセージを出力してここでの処理を終了する（ステップ1625）。

【0081】（3）ステップ1610のチェックで、交換テーブルに受信側VPN-IDがあれば、検索によって見つかった交換情報のフラグを「削除承認待ち」に変更し、そして、仮削除完了を表すACKメッセージを相手サービス事業者側の相互接続装置に対して管理用回線経由で送信して処理を終了する（ステップ1615、1620）。

【0082】図17は管理者の登録承認を受けた相互接続装置における交換情報登録完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図5において、相互接続装置110-Bが、シーケンス530で管理者の登録承認を受けてからシーケンス550で登録完了メッセージを送信するまでの処理に相当する。

【0083】（1）ネットワーク管理者による登録承認を入力された相互接続装置は、その入力に含まれる自サービス事業者側VPN-IDが交換テーブルにすでに登

録されているか否かを検索し、検索の結果、自サービス事業者側VPN-IDがすでに交換テーブルに登録されているか否かをチェックする（ステップ1705、1710）。

【0084】（2）ステップ1710のチェックで、もし交換テーブルに自サービス事業者側VPN-IDがなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ1740）。

10 【0085】（3）ステップ1710のチェックで、交換テーブルに自サービス事業者側VPN-IDがあれば、見つかったその交換情報のフラグが「登録承認待ち」になっているか否かをチェックし、フラグが「登録承認待ち」でなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する（ステップ1715、1740）。

【0086】（4）ステップ1715のチェックで、見つかった交換情報のフラグが「登録承認待ち」であれば、見つかった交換情報の登録承認時に入力された自サービス事業者側の境界ルータのIPアドレス及び自サービス事業者側相互接続装置のI/F識別子をその交換情報に登録する。但し、自サービス事業者側の境界ルータのIPアドレスについては、管理者による入力時に変更が特になければ、相手サービス事業者側の相互接続装置から送られてきた値がそのまま使用される。また、境界ルータのIPアドレスとI/F識別子については、相互接続装置が適切な値を自動的に決定してもよい（ステップ1720）。

30 【0087】（5）次に、自サービス事業者側の境界ルータに対して、自サービス事業者側と相手サービス事業者側との境界ルータのIPアドレス、境界ルータ間接続のIPネットマスク、その他ルーティング情報交換のための設定を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が登録承認入力を行う前に、他の手段により境界ルータに対して直接この設定を行ってもよい（ステップ1725）。

40 【0088】（6）そして、対象となっている交換情報のフラグを「有効」に変更し、相手サービス事業者側の相互接続装置へ登録完了メッセージを送信する。この登録完了メッセージの各フィールドには、対象となっている交換情報の各フィールドの値を用いる（ステップ1730、1735）。

50 【0089】図18は管理者の削除承認を受けた相互接続装置における交換情報削除完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、図6において、相互接続装置110-Bが、シーケンス640で管理者の削除承認を受けてから、削除を要求された情報を変換テーブル325から削除するまでの処理に相当する。

【0090】(1) ネットワーク管理者による削除承認が入力された相互接続装置は、その入力に含まれる自サービス事業者側VPN-IDが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側VPN-IDがすでに変換テーブルに登録されているか否かをチェックする(ステップ1805、1810)。

【0091】(2) ステップ1810のチェックで、もし変換テーブルに自サービス事業者側VPN-IDがなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する(ステップ1830)。

【0092】(3) ステップ1810のチェックで、変換テーブルに自サービス事業者側VPN-IDがあれば、見つかったその変換情報のフラグが「削除承認待ち」か否かをチェックし、フラグが「削除承認待ち」でなければネットワーク管理者が使用しているディスプレイモニタへエラーを出力してここでの処理を終了する(ステップ1815、1830)。

【0093】(4) ステップ1815のチェックで、フラグが「削除承認待ち」であれば、自サービス事業者側の境界ルータに対して、変換情報に含まれる各種情報(自サービス事業者側と相手サービス事業者側の境界ルータのIPアドレス、境界ルータ間接続のIPネットマスク)やその他ルーティング情報交換のための設定の解除要求を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が削除承認入力を行う前に、他の手段で境界ルータに対して直接この設定解除を行ってもよい(ステップ1820)。

【0094】(5) そして、ネットワーク管理者による削除承認が入力された相互接続装置は、対象となっている変換情報を完全に削除して処理を終了する(ステップ1825)。

【0095】図19は登録完了メッセージを受信した相互接続装置における変換情報登録完了の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、例えば、前述した図5において、相互接続装置110-Aが、シーケンス550で登録完了メッセージを受信してからシーケンス570でACKメッセージを送信するまでの処理に相当する。

【0096】(1) 相手サービス事業者側の相互接続装置から登録完了メッセージを受信した相互接続装置は、その入力に含まれる自サービス事業者側VPN-IDが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側VPN-IDがすでに変換テーブルに登録されているか否かをチェックする(ステップ1905、1910)。

【0097】(2) ステップ1910のチェックで、もし変換テーブルに自サービス事業者側VPN-IDがな

ければ、相手サービス事業者側の相互接続装置へ「該当する登録完了待ち変換情報なし」のエラーを表すNOTIFYメッセージを出力してここでの処理を終了する(ステップ1945)。

【0098】(3) また、ステップ1910のチェックで、変換テーブルに自サービス事業者側VPN-IDがあれば、見つかった変換情報のフラグが「登録完了待ち」か否かをチェックし、フラグが「登録完了待ち」でなければ、前述と同様にNOTIFYメッセージを出力してここでの処理を終了する(ステップ1915、1945)。

【0099】(4) また、ステップ1915のチェックで、フラグが「登録完了待ち」であれば、見つかった変換情報のシーケンス番号が受信した登録完了メッセージ内の仮設定シーケンス番号と一致するか否かをチェックし、一致しなければ、前述と同様にNOTIFYメッセージを出力してここでの処理を終了する(ステップ1920、1945)。

【0100】(5) ステップ1920のチェックで、見つかった変換情報のシーケンス番号が受信した登録完了メッセージ内の仮設定シーケンス番号と一致した場合、すなわち、ステップ1910、1915、1920のチェックにより該当する変換情報が見つかった場合、受信した登録完了メッセージに含まれる送信側の境界ルータのIPアドレスと、該当する変換情報の相手サービス事業者側境界ルータのIPアドレスとを比較する。その結果、値が異なるか、あるいは変換情報側のこれらのフィールドが未登録である場合、メッセージ内のこれらの値を変換情報側へコピーして、相手側境界ルータのIPアドレスを登録し、対象となっている変換情報のフラグを「有効」に変更する(ステップ1925、1930)。

【0101】(6) 次に、自サービス事業者側の境界ルータに対して、自サービス事業者側と相手サービス事業者側との境界ルータのIPアドレス、境界ルータ間接続のためのIPネットマスク、その他ルーティング情報交換のための設定を送信する。但し、自サービス事業者側の境界ルータが相互接続装置からの設定送信による設定変更に対応できない場合、ネットワーク管理者が図13の仮登録処理の前に行った登録要求入力を行う前に、他の手段により境界ルータに対して直接この設定を行ってもよい(ステップ1935)。

【0102】(7) 最後に、登録完了を表すACKメッセージを相手サービス事業者側の相互接続装置へ管理用回線経由で送信して処理を終了する(ステップ1940)。

【0103】図20はACKメッセージを受信した相互接続装置における各種の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図5のシーケンス520及び570、あるいは、図6のシーケンス630で送信されたACKメッセージを

受け取った相互接続装置の処理である。

【0104】(1) 相手サービス事業者側の相互接続装置からACKメッセージを受信した相互接続装置は、受信したACKメッセージに含まれる自サービス事業者側VPN-IDが変換テーブルにすでに登録されているか否かを検索し、検索の結果、自サービス事業者側VPN-IDがすでに変換テーブルに登録されているか否かをチェックする(ステップ2005、2010)。

【0105】(2) ステップ2010のチェックで、もし変換テーブルに自サービス事業者側VPN-IDがなければ、相手サービス事業者側の相互接続装置へ「該当する変換情報なし」のエラーを表すNOTIFYメッセージを出力してここでの処理を終了する。(ステップ2025)。

【0106】(3) また、ステップ2010のチェックで、変換テーブルに自サービス事業者側VPN-IDがあれば、その変換情報のシーケンス番号が受信したACKメッセージ内の返答対象シーケンス番号と一致するか否かをチェックし、一致しなければ、前述と同様にNOTIFYメッセージを出力してここでの処理を終了する(ステップ2015、2025)。

【0107】(4) ステップ2015のチェックで、変換情報のシーケンス番号が受信したACKメッセージ内の返答対象シーケンス番号と一致すれば、その変換情報のフラグが「仮登録返答待ち」か否かをチェックし、フラグが「仮登録返答待ち」でなければ、何も行わずにこの処理を終了する(ステップ2020)。

【0108】(5) ステップ2020のチェックで、フラグが「仮登録返答待ち」であれば、そのフラグを「登録完了待ち」に変更して処理を終了する(ステップ2030)。

【0109】図21は自サービス事業者側からデータパケットを受信した相互接続装置がそのパケットを外部に送信する外部送信処理の動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図7に示すシーケンス700、710により説明した境界ルータ120-Aからのデータパケットを受信した相互接続装置110-Aが、相互接続装置110-Bにパケットを送信する処理である。

【0110】(1) 境界ルータからデータパケットを受信した相互接続装置は、そのデータパケットの先頭に置かれている自サービス事業者内通信用ヘッダを見て、そのヘッダに含まれるVPN-IDが変換テーブルにすでに登録されているか否かを検索し、検索の結果、そのVPN-IDがすでに変換テーブルに登録されているか否かをチェックする(ステップ2105、2110)。

【0111】(2) ステップ2110のチェックで、もし変換テーブルに該当VPN-IDがなければ、そのパケットを破棄してここでの処理を終了する(ステップ2130)。

【0112】(3) また、ステップ2110のチェックで、変換テーブルに該当VPN-IDがあれば、その変換情報のフラグが「有効」か否かをチェックし、フラグが「有効」でなければ、前述と同様にパケットを破棄してここでの処理を終了する(ステップ2115、2130)。

【0113】(4) ステップ2115のチェックで、変換情報のフラグが有効であれば、そのパケットから自サービス事業者内通信用ヘッダを取り除いてIPパケットを取り出し、そのIPパケットを検索によって見つかった変換情報に含まれるI/F識別子で表されるデータ用回線インタフェースへ出力することにより、相手サービス事業者側の相互接続装置へパケットを送信して処理を終了する(ステップ2120、2125)。

【0114】図22は相手のサービス事業者側からデータパケットを受信した相互接続装置における内部送信の処理動作を説明するフローチャートであり、以下、これについて説明する。この処理は、図7に示すシーケンス710、720により説明した相互接続装置110-Aからのデータパケットを受信した相互接続装置110-Bが、境界ルータ120-Bにパケットを送信する処理である。

【0115】(1) 相手サービス事業者側の相互接続装置からデータ用回線を通してIPデータパケットを受信した相互接続装置は、そのデータパケットを受信したデータ用回線のI/F識別子が変換テーブルにすでに登録されているか否かを検索し、検索の結果、そのI/F識別子が既に変換テーブルに登録されているか否かをチェックする(ステップ2205、2210)。

【0116】(2) ステップ2210のチェックで、もし変換テーブルに該当I/F識別子がなければ、そのパケットを破棄してここでの処理を終了する(ステップ2230)。

【0117】(3) また、ステップ2210のチェックで、変換テーブルに該当I/F識別子があった場合、その変換情報のフラグが「有効」か否かをチェックし、フラグが「有効」でなければ、前述と同様にパケットを破棄してここでの処理を終了する(ステップ2215、2230)。

【0118】(4) ステップ2215のチェックで、変換情報のフラグが有効であれば、その変換情報に含まれる自サービス事業者側VPN-IDを含む自サービス事業者内通信用ヘッダを受信したIPパケットに付加し、そのパケットを境界ルータ側の回線へ送信する(ステップ2220、2225)。

【0119】

【発明の効果】前述したように、本発明の実施形態によれば、相互接続装置を利用して異なるVPNの方式を用いている2つのサービス事業者の間で、複数のVPNを相互に接続することができる。そして、本発明の実施形

態による相互接続装置は、管理情報を交換することによって転送するVPNの設定を行っているため、ネットワーク管理者の手間を軽減することができる。また、相互接続時の相互接続装置間の回線には、通常のIPパケットが流れることになるため、一方のサービス事業者が内部での複数VPN運用を提供していない場合は、通常のIPネットワーク機器を接続することによって特定のVPN-IDに限ってIPパケットを送受信することができる。これらの結果、本発明の実施形態によれば、複数のサービス事業者が互いのVPNを効率良く相互接続することができる。

#### 【0120】

【発明の効果】以上説明したように本発明によれば、異なるサービス事業者のVPN相互を効率的に接続することを可能にした相互接続装置及びこれを用いたネットワークシステムを提供することができる。

#### 【図面の簡単な説明】

【図1】本発明の相互接続装置を用いてサービス事業者間のVPN相互接続を行うネットワークシステムの構成例を示すブロック図である。

【図2】本発明の一実施形態による相互接続装置のハードウェア構成を示すブロック図である。

【図3】本発明の一実施形態による相互接続装置のソフトウェア構成を説明する図である。

【図4】本発明の一実施形態による相互接続装置が使用する変換テーブルの構成を説明する図である。

【図5】相互接続装置相互間のVPN変換情報の登録シーケンスを示す図である。

【図6】相互接続装置相互間のVPN変換情報の削除シーケンスを示す図である。

【図7】相互接続装置相互間でのデータパケットの送受信シーケンスを示す図である。

【図8】VPN変換情報を登録しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する登録メッセージの形式を示す図である。

【図9】登録メッセージを受信した相互接続装置が登録メッセージを送信してきた相互接続装置へ返信する登録完了メッセージの形式を示す図である。

【図10】VPN変換情報を削除しようとしたサービス事業者側の相互接続装置が他方の相互接続装置へ送信する削除メッセージの形式を示す図である。

【図11】メッセージを受け取った相互接続装置が相手の相互接続装置へ返答する受信確認(ACK)メッセージの形式を示す図である。

【図12】メッセージの受け取り時にエラーが発生した場合に相手の相互接続装置へ送信する異常通知(NOTIFY)メッセージの形式を示す図である。

【図13】VPN変換情報を登録しようとしたサービス事業者側の相互接続装置における変換情報仮登録の処理動作を説明するフローチャートである。

【図14】VPN変換情報を削除しようとしたサービス事業者側の相互接続装置における変換情報削除の処理動作を説明するフローチャートである。

【図15】登録メッセージを受信した相互接続装置における変換情報仮登録の処理動作を説明するフローチャートである。

【図16】削除メッセージを受信した相互接続装置における変換情報仮削除の処理動作を説明するフローチャートである。

10 【図17】管理者の登録承認を受けた相互接続装置における変換情報登録完了の処理動作を説明するフローチャートである。

【図18】管理者の削除承認を受けた相互接続装置における変換情報削除完了の処理動作を説明するフローチャートである。

【図19】登録完了メッセージを受信した相互接続装置における変換情報登録完了の処理動作を説明するフローチャートである。

20 【図20】ACKメッセージを受信した相互接続装置における各種の処理動作を説明するフローチャートである。

【図21】自サービス事業者側からデータパケットを受信した相互接続装置がそのパケットを外部に送信する外部送信処理の動作を説明するフローチャートである。

【図22】相手のサービス事業者側からデータパケットを受信した相互接続装置における内部送信の処理動作を説明するフローチャートである。

#### 【符号の説明】

100-A、100-B サービス事業者ネットワーク  
30 110-A、110-B 相互接続装置  
120-A、120-B 境界ルータ  
130 データ用回線  
140 管理用回線  
200 CPU(Central Processing Unit)  
210 メモリ  
213 オペレーティングシステム(OS)  
215 制御ソフト  
220 内部ネットワークコントローラ  
225 外部ネットワークコントローラ  
230 キーボードコントローラ  
235 キーボード  
240 シリアルコントローラ  
245 マウス  
250 ディスプレイコントローラ  
255 ディスプレイモニタ  
260 ディスクコントローラ  
265 ディスク装置  
310 入出力制御部  
320 変換管理テーブル  
50 325 変換テーブル

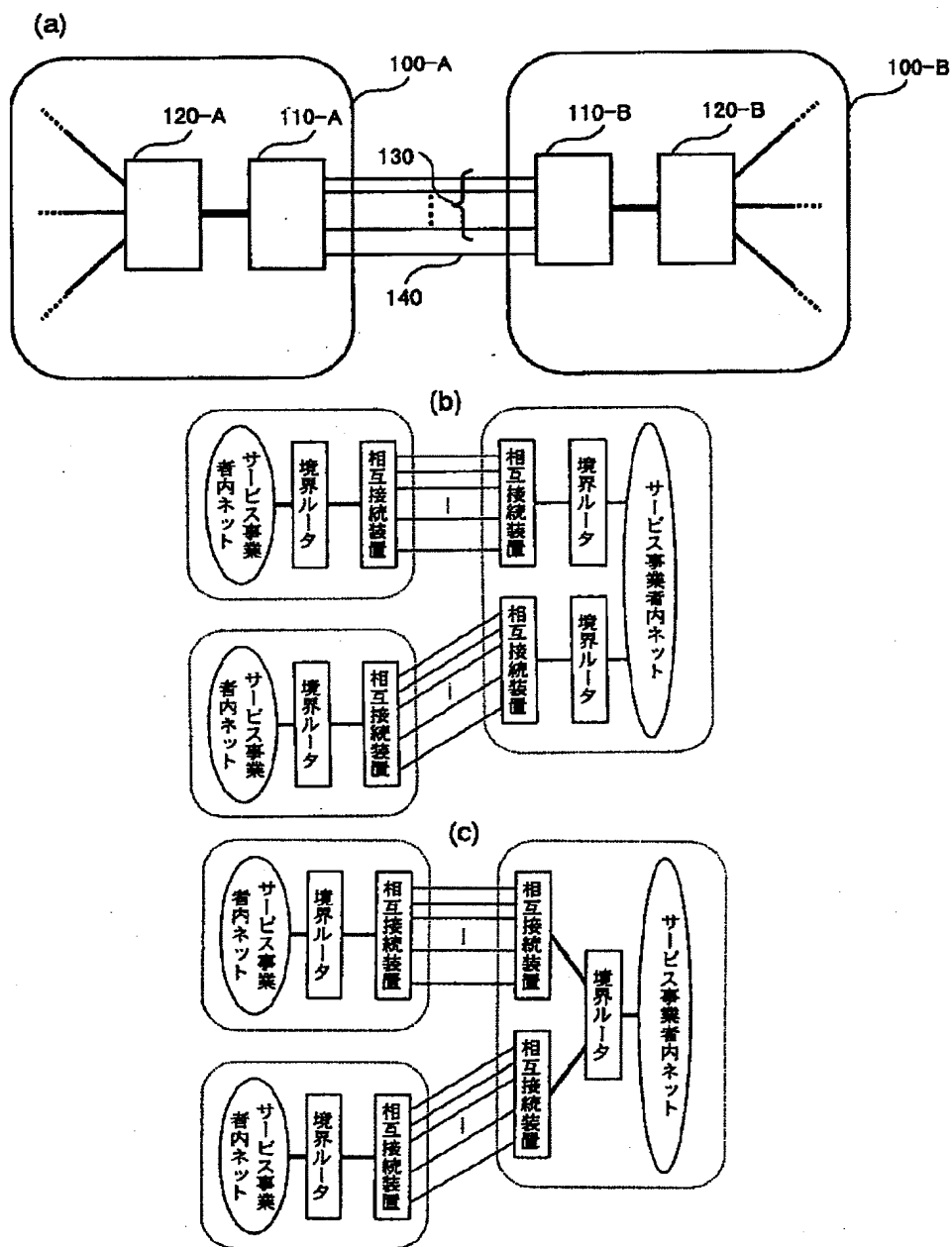


330 境界ルータ接続設定部  
 340 データ中継部  
 350 管理情報送受信部  
 360 境界ルータ通信部

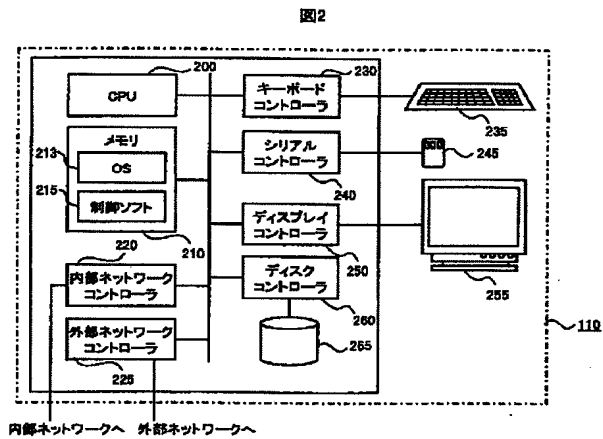
370 外部回線通信部  
 380 内部ネットワークインタフェース部  
 390 外部ネットワークインタフェース部

【図1】

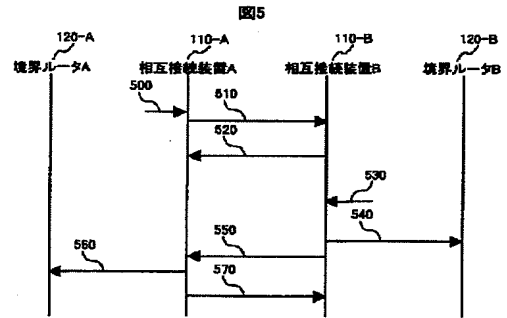
図1



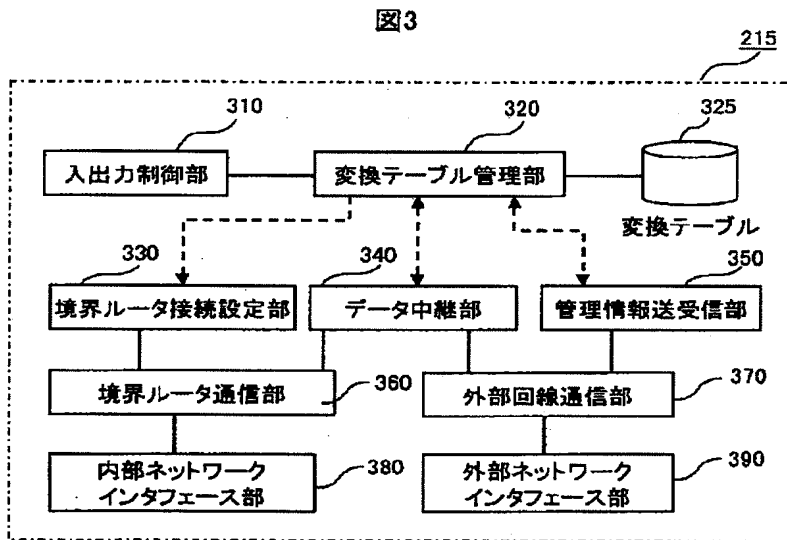
【図2】



【図5】



【図3】



【図4】

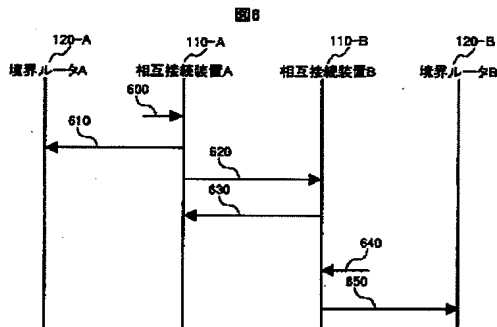
図4

図4

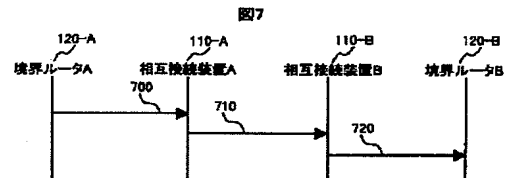
VPN-ID	相手VPN-ID	接続ネットマスク	ルータアドレス	相手ルータアドレス	V/F識別子	シーケンス番号	フラグ

410 420 430 440 450 460 470 480

【図6】

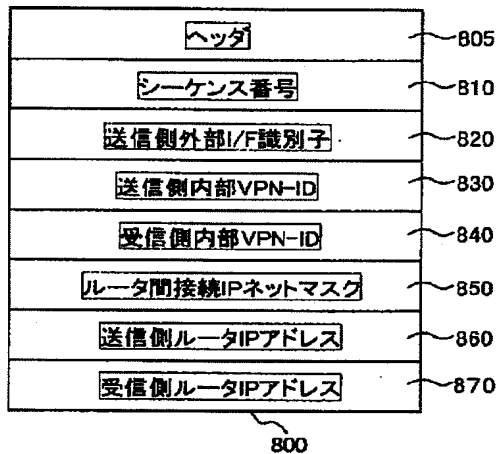


【図7】



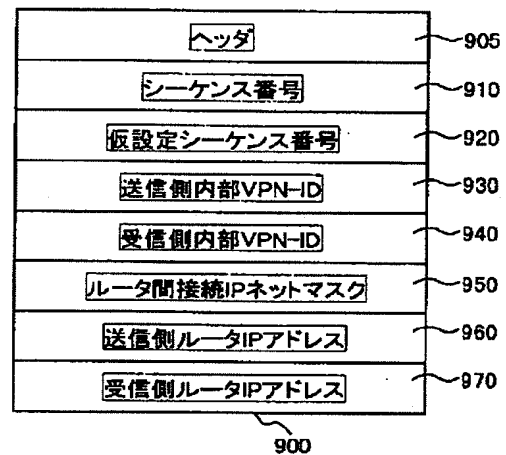
【図8】

図8



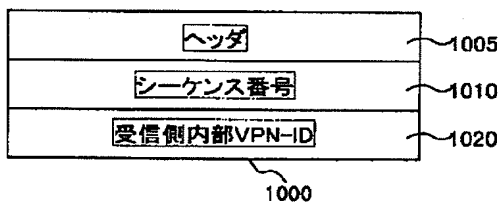
【図9】

図9



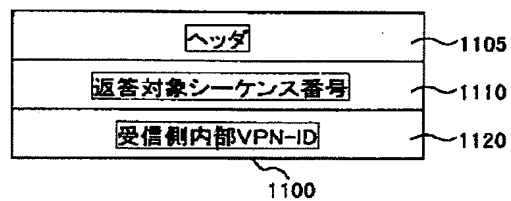
【図10】

図10



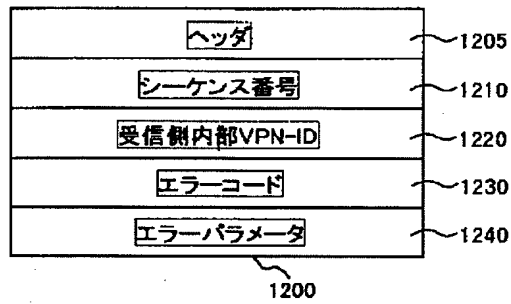
【図11】

図11



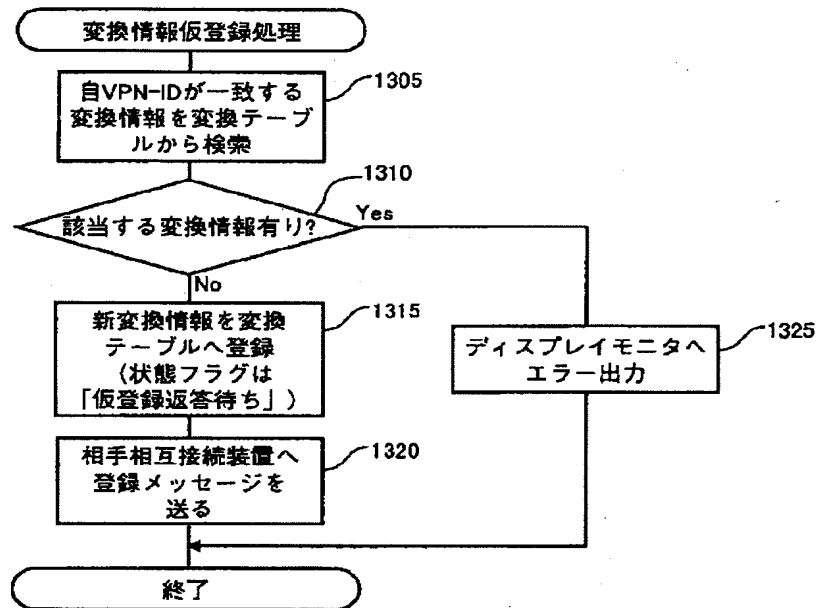
【図12】

図12



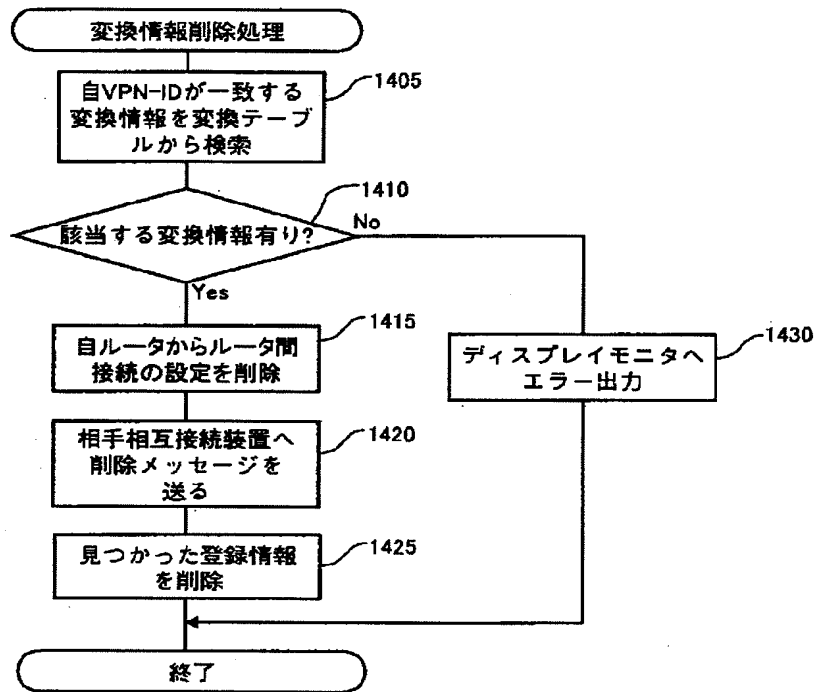
【図13】

図13



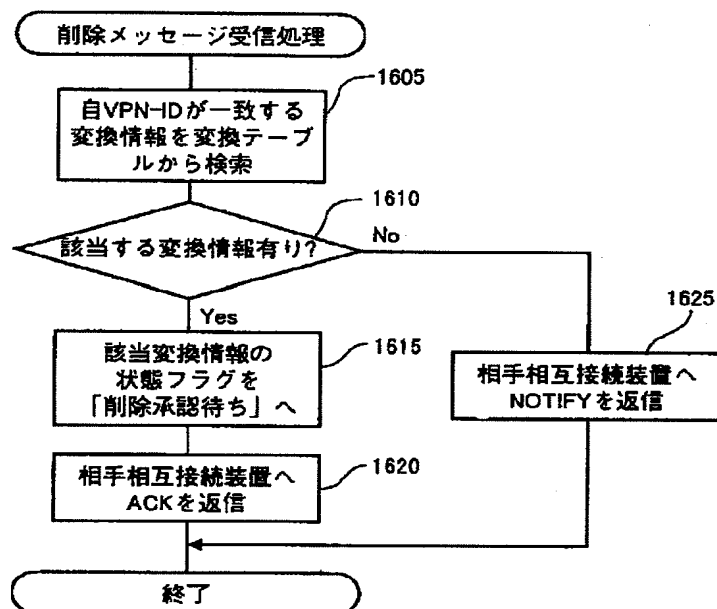
【図14】

図14



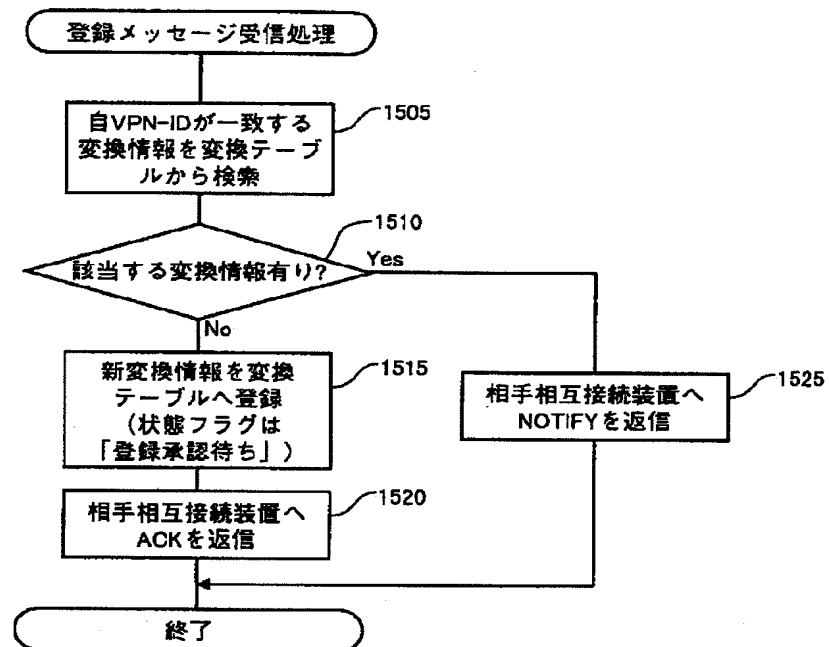
【図16】

図16



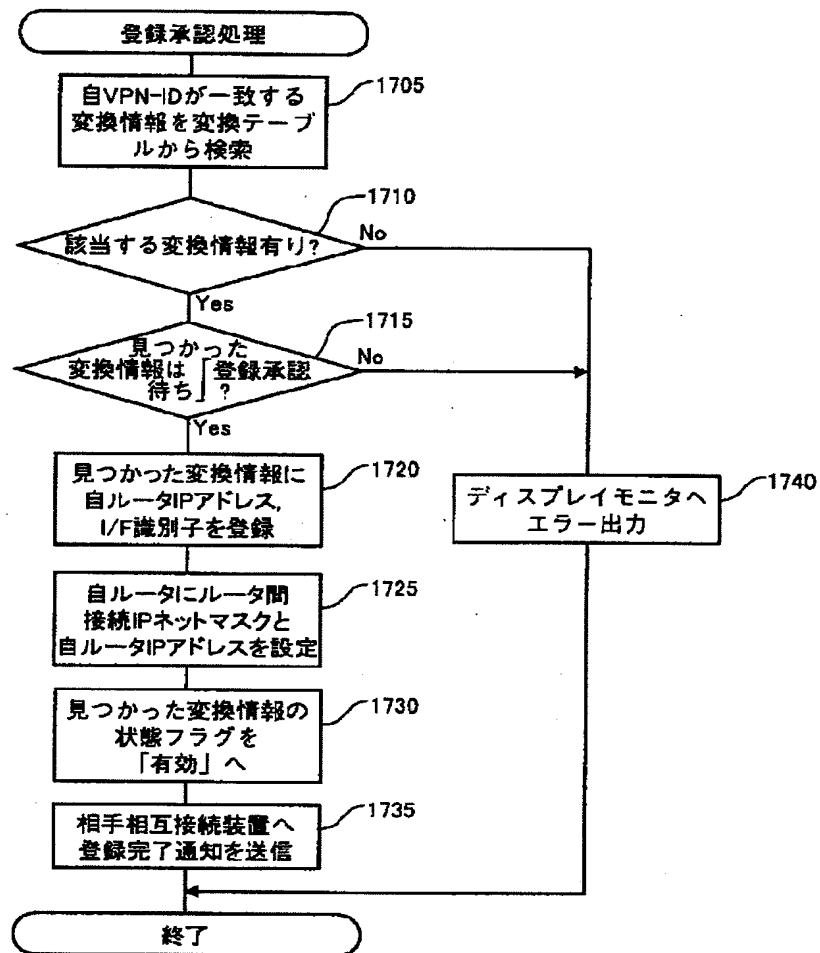
【図15】

図15



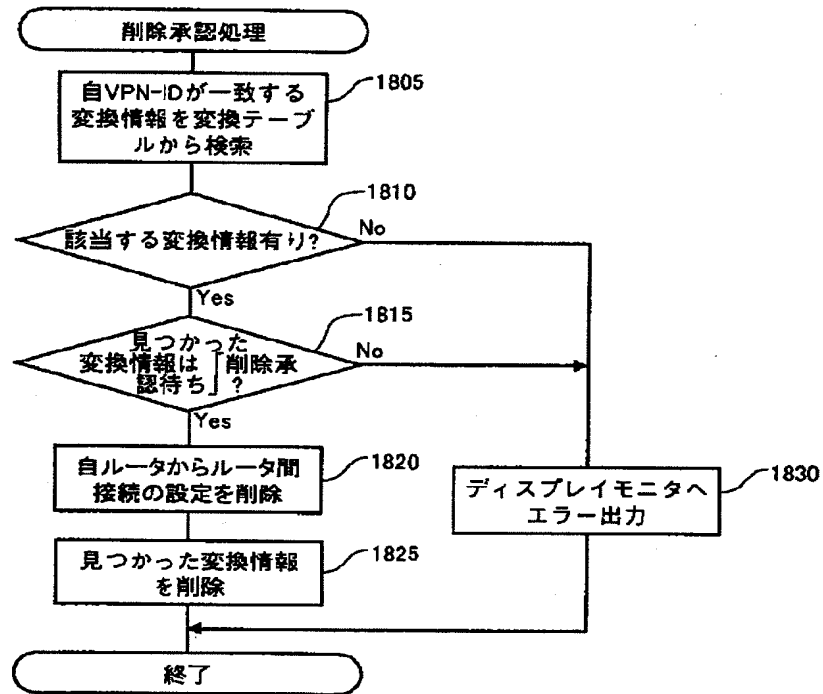
【図17】

図17



【図18】

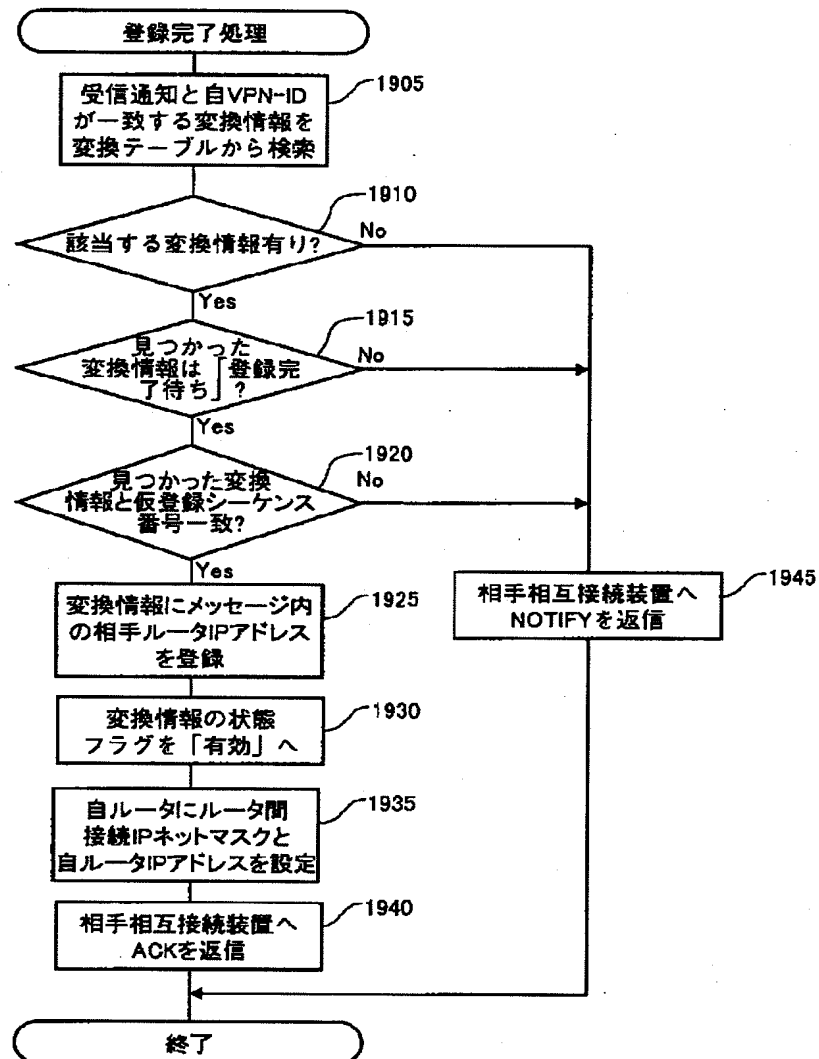
図18





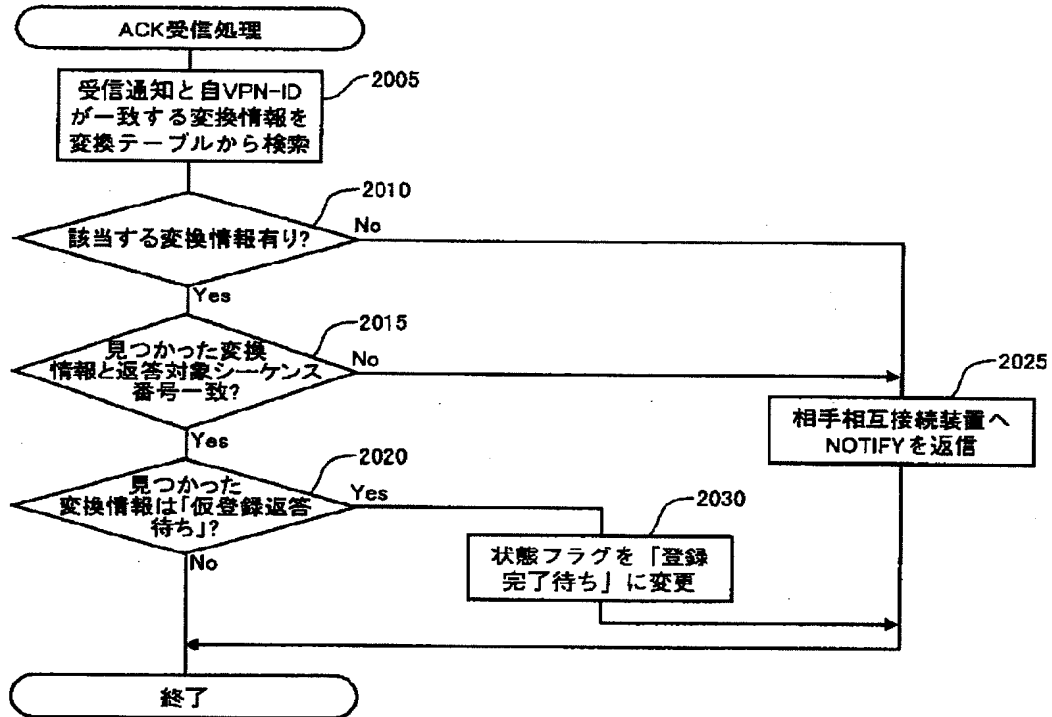
【図19】

図19



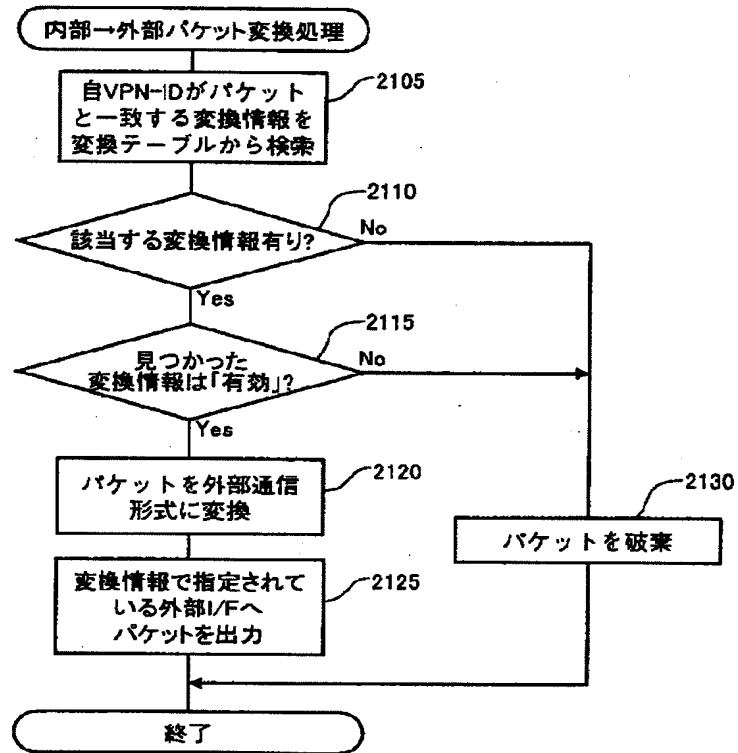
【図20】

図20



【図21】

図21



【図22】

図22

